特　許　協　力　条　約

PCT

国際予備審査報告

（法第１２条、法施行規則第56条）
〔ＰＣＴ３６条及びＰＣＴ規則70〕

出願人又は代理人の書類記号　１００２８	今後の手続きについては、国際予備審査報告の送付通知（様式ＰＣＴ／ＩＰＥＡ／４１６）を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ０３／０７７９４	国際出願日（日.月.年）　１９．０６．２００３	優先日（日.月.年）　１９．０６．２００２
国際特許分類（ＩＰＣ） Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ９／３２		
出願人（氏名又は名称） 株式会社エイシーエス		

１．　国際予備審査機関が作成したこの国際予備審査報告を法施行規則第57条（ＰＣＴ３６条）の規定に従い送付する。

２．　この国際予備審査報告は、この表紙を含めて全部で　9　ページからなる。

[X]　この国際予備審査報告には、附属書類、つまり補正されて、この報告の基礎とされた及び／又はこの国際予備審査機関に対してした訂正を含む明細書、請求の範囲及び／又は図面も添付されている。
（ＰＣＴ規則70.16及びＰＣＴ実施細則第６０７号参照）
この附属書類は、全部で　2　ページである。

３．　この国際予備審査報告は、次の内容を含む。

- Ⅰ　[X]　国際予備審査報告の基礎
- Ⅱ　[ ]　優先権
- Ⅲ　[X]　新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成
- Ⅳ　[X]　発明の単一性の欠如
- Ⅴ　[X]　ＰＣＴ３５条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明
- Ⅵ　[ ]　ある種の引用文献
- Ⅶ　[ ]　国際出願の不備
- Ⅷ　[X]　国際出願に対する意見

国際予備審査の請求書を受理した日　１９．０６．２００３	国際予備審査報告を作成した日　１９．０２．２００４
名称及びあて先 日本国特許庁（ＩＰＥＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　5M　9364 中里　裕正 電話番号　０３－３５８１－１１０１　内線　３５９７

様式ＰＣＴ／ＩＰＥＡ／４０９（表紙）（１９９８年７月）

国際予備審査報告

国際出願番号　ＰＣＴ／ＪＰ０３／０７７９４

Ⅰ．　国際予備審査報告の基礎

1．　この国際予備審査報告は下記の出願書類に基づいて作成された。（法第６条（ＰＣＴ１４条）の規定に基づく命令に応答するために提出された差し替え用紙は、この報告書において「出願時」とし、本報告書には添付しない。ＰＣＴ規則70.16, 70.17）

☐ 出願時の国際出願書類

☒ 明細書　第 1-36, 38-70 ページ、　出願時に提出されたもの
明細書　第 　　ページ、　国際予備審査の請求書と共に提出されたもの
明細書　第 37 ページ、　09.02.2004 付の書簡と共に提出されたもの

☒ 請求の範囲　第 1-26, 28-50 項、　出願時に提出されたもの
請求の範囲　第 　　項、　ＰＣＴ１９条の規定に基づき補正されたもの
請求の範囲　第 　　項、　国際予備審査の請求書と共に提出されたもの
請求の範囲　第 27 項、　09.02.2004 付の書簡と共に提出されたもの

☒ 図面　第 1-16 ~~ページ~~図、　出願時に提出されたもの
図面　第 　　ページ／図、　国際予備審査の請求書と共に提出されたもの
図面　第 　　ページ／図、　　付の書簡と共に提出されたもの

☐ 明細書の配列表の部分　第 　　ページ、　出願時に提出されたもの
明細書の配列表の部分　第 　　ページ、　国際予備審査の請求書と共に提出されたもの
明細書の配列表の部分　第 　　ページ、　　付の書簡と共に提出されたもの

2．　上記の出願書類の言語は、下記に示す場合を除くほか、この国際出願の言語である。

上記の書類は、下記の言語である 　　語である。

☐ 国際調査のために提出されたＰＣＴ規則23.1(b)にいう翻訳文の言語
☐ ＰＣＴ規則48.3(b)にいう国際公開の言語
☐ 国際予備審査のために提出されたＰＣＴ規則55.2または55.3にいう翻訳文の言語

3．　この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際予備審査報告を行った。

☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出された磁気ディスクによる配列表
☐ 出願後に、この国際予備審査（または調査）機関に提出された書面による配列表
☐ 出願後に、この国際予備審査（または調査）機関に提出された磁気ディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった
☐ 書面による配列表に記載した配列と磁気ディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

4．　補正により、下記の書類が削除された。
☐ 明細書　第 　　ページ
☐ 請求の範囲　第 　　項
☐ 図面　図面の第 　　ページ／図

5．☐ この国際予備審査報告は、補充欄に示したように、補正が出願時における開示の範囲を越えてされたものと認められるので、その補正がされなかったものとして作成した。（ＰＣＴ規則70.2(c)　この補正を含む差し替え用紙は上記１．における判断の際に考慮しなければならず、本報告に添付する。）

国際予備審査報告

国際出願番号　ＰＣＴ／ＪＰ０３／０７７９４

Ⅲ．　新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成

１．次に関して、当該請求の範囲に記載されている発明の新規性、進歩性又は産業上の利用可能性につき、次の理由により審査しない。

☐ 国際出願全体

☒ 請求の範囲 1-13, 27

理由：

☐ この国際出願又は請求の範囲 _____ は、国際予備審査をすることを要しない次の事項を内容としている（具体的に記載すること）。

☒ 明細書、請求の範囲若しくは図面（次に示す部分）又は請求の範囲 1-13 の記載が、不明確であるため、見解を示すことができない（具体的に記載すること）。

別紙を参照されたい。

☐ 全部の請求の範囲又は請求の範囲 _____ が、明細書による十分な裏付けを欠くため、見解を示すことができない。

☒ 請求の範囲 1-13, 27 について、国際調査報告が作成されていない。

２．ヌクレオチド又はアミノ酸の配列表が実施細則の附属書Ｃ（塩基配列又はアミノ酸配列を含む明細書等の作成のためのガイドライン）に定める基準を満たしていないので、有効な国際予備審査をすることができない。

☐ 書面による配列表が提出されていない又は所定の基準を満たしていない。

☐ 磁気ディスクによる配列表が提出されていない又は所定の基準を満たしていない。

国際予備審査報告

国際出願番号　ＰＣＴ／ＪＰ０３／０７７９４

Ⅳ．　発明の単一性の欠如

1．　請求の範囲の減縮又は追加手数料の納付の求めに対して、出願人は、

☐ 請求の範囲を減縮した。

☐ 追加手数料を納付した。

☐ 追加手数料の納付と共に異議を申立てた。

☐ 請求の範囲の減縮も、追加手数料の納付もしなかった。

2．☒ 国際予備審査機関は、次の理由により発明の単一性の要件を満たしていないと判断したが、ＰＣＴ規則68.1の規定に従い、請求の範囲の減縮及び追加手数料の納付を出願人に求めないこととした。

3．　国際予備審査機関は、ＰＣＴ規則13.1、13.2及び13.3に規定する発明の単一性を次のように判断する。

☐ 満足する。

☒ 以下の理由により満足しない。

請求の範囲1-13は、ワンタイムＩＤとは何ら関係しない相互認証に関する発明であり、請求の範囲14-50は、ワンタイムＩＤに関する発明である。なお、相互認証は周知の技術であるから、相互認証を「特別な技術的特徴」とすることはできない。

4．　したがって、この国際予備審査報告書を作成するに際して、国際出願の次の部分を、国際予備審査の対象にした。

☐ すべての部分

☒ 請求の範囲 14-26, 28-50 に関する部分

国際予備審査報告	国際出願番号　ＰＣＴ／ＪＰ０３／０７７９４

Ｖ．　新規性、進歩性又は産業上の利用可能性についての法第１２条（ＰＣＴ３５条(2)）に定める見解、それを裏付ける文献及び説明

１．　見解

新規性（N）	請求の範囲	14, 15, 17, 18, 20-24, 26, 28-43, 47-50	有
	請求の範囲	16, 19, 25, 44-46	無
進歩性（ＩＳ）	請求の範囲	14, 15, 17, 18, 20-24, 26, 28-43, 47-50	有
	請求の範囲	16, 19, 25, 44-46	無
産業上の利用可能性（ＩＡ）	請求の範囲	14-26, 28-50	有
	請求の範囲		無

２．　文献及び説明（ＰＣＴ規則70.7）

請求の範囲16, 19, 25, 44-46は、国際調査報告で引用された文献１（HANDBOOK of APPLIED CRYPTOGRAPHY, CRC Press, 1997, p. 400-403）により新規性を有しない。引用文献１には「Ｂが、チャレンジr_BをＡに送信し、
Ａが、上記チャレンジr_Bと共有鍵Ｋを引数とする一方向性関数値h_K（…r_B…）を求め、この一方向性関数値h_K（…r_B…）とチャレンジr_AをＢに送信し、
Ｂが、上記チャレンジr_Bと共有鍵Ｋを引数とする一方向性関数値h_K（…r_B…）を求め、この値とＡから受信した一方向性関数値h_K（…r_B…）との比較により、Ａの正当性を判定すると共に、
Ｂが、上記チャレンジr_A, r_Bと共有鍵Ｋを引数とする一方向性関数値h_K（r_B, r_A, …）を求め、この値をＡに送信し、
Ａが、上記チャレンジr_A, r_Bと共有鍵Ｋを引数とする一方向性関数値h_K（r_B, r_A, …）を求め、この値とＡから受信した一方向性関数値h_K（r_B, r_A, …）との比較により、Ｂの正当性を判定する認証方法」に係る発明が記載されている。
チャレンジが一回ごとに生成される乱数であることは技術常識であるから、一方向性関数値もまた一回限りの情報である。そして、VIII欄にて述べるように、これらの請求の範囲に記載された「ワンタイムＩＤ」とは一般にいう「ＩＤ」であるとは認められず、むしろエンティテイの正当性を判定するための情報であるから、引用文献１に記載された発明における一方向性関数値と、これら請求の範囲に記載された「ワンタイムＩＤ」との間に格別の相違があるとは認められない。また同じく後述するように、「第一のワンタイムＩＤ」を生成送信することは、その意義が不明なものであるから、かかる工程を有することに格別なものがあるとも認められない。

請求の範囲14, 15, 17, 18, 20-24, 26, 28-43, 47-50は、新規性および進歩性を有する。これらの請求の範囲に記載された発明は、引用文献に記載も示唆もされていない。

Ⅷ.　国際出願に対する意見

請求の範囲、明細書及び図面の明瞭性又は請求の範囲の明細書による十分な裏付についての意見を次に示す。

（ａ）明細書又は図面に実施の形態１の例として記載されたものは、第三者によるなりすましが可能であり、実質的に認証として機能しない。以下に説明する。
クライアント・サーバ間で通信されるデータには、以下の関係式が成り立つ。

$S_{n+1} = C_{n+1} + Q_n$, $C_{n+1} = S_n + R_n$, $A_n = R_n + K_{n-1}$, $B_n = Q_n + K_{n-1}$

これら４つの関係式より、以下の２式が成り立つ。

$S_{n+1} - S_n = Q_n + R_n$, $A_n - B_n = -Q_n + R_n$

したがって、以下の式によりQ_n 及び R_n を計算することができる。

$Q_n = (S_{n+1} - S_n - A_n + B_n)/2$, $R_n = (S_{n+1} - S_n + A_n - B_n)/2$

ここで、S_{n+1}, S_n, A_n, B_n は全てクライアント・サーバ間の通信路に現れるデータであるから、第三者がそれらを傍受してQ_n 及び R_n を求めることが可能である。そしてC_n 及び S_n も通信路上に現れるから、第三者がそれらQ_n, R_n, C_n, S_n を用いてK_n を求めることもできる。したがって、以下の式によりQ_{n+1} 及び R_{n+1} を計算することができる。

$Q_{n+1} = B_{n+1} - K_n$, $R_{n+1} = A_{n+1} - K_n$

これらQ_{n+1} 及び R_{n+1} と、通信路上に現れるC_{n+1} 及び S_{n+1} を用いて、K_{n+1} を求めることもできる。すなわち、通信路上に現れるデータを観測するのみで任意の隠蔽鍵を計算することができる。このことは、任意の第三者がクライアントあるいはサーバの双方に対してなりすましができることを意味し、この実施の形態１の例に記載されたものは、実質的に相互認証たり得ない。

補充欄（いずれかの欄の大きさが足りない場合に使用すること）

第　Ⅷ　欄の続き

（ｂ）実施の形態２には、ステップＳ２において、サーバがＳＩＧＮＡＬを演算により求めることが記載されている。ここでＳＩＧＮＡＬ$_i$の演算には鍵Ｋ$_{i-1}$が必要であり、鍵Ｋ$_{i-1}$の演算には、サーバ・クライアント間の任意の共有鍵、ＤＨ共通鍵g^{xy}、ＳＩＧＮＡＬ$_{i-1}$の３つが必要である。しかしながら明細書の記載を参照しても、ＤＨ共通鍵g^{xy}については記憶装置１３に格納することが記載されているが、ＳＩＧＮＡＬ$_{i-1}$については特に記憶することが記載されておらず、ＳＩＧＮＡＬ$_{i-1}$をどのようにして得るのか不明である。また、ＳＩＧＮＡＬ$_{i-1}$も記憶装置に記憶されているとしても、これらＤＨ共通鍵g^{xy}及びＳＩＧＮＡＬ$_{i-1}$を演算に用いるに当たって、以下の点が不明である。すなわち一般に、サーバには複数のクライアントが接続されるものであり、その場合、ＤＨ共通鍵g^{xy}及びＳＩＧＮＡＬ$_{i-1}$はクライアント毎に異なるものと認められる。そうすると、サーバにおいてこれらのデータを用いる際には、複数のクライアントにそれぞれ対応した複数組のデータのなかから、接続を要求したクライアントに対応するデータを選択しなければならない。しかしながら、クライアントから送信されるＳＩＧＮＡＬ$_i$は接続する毎に変化するデータであり、それによりクライアントを特定することはできない。そうすると、サーバが鍵Ｋ$_{i-1}$ひいてはＳＩＧＮＡＬ$_i$を計算するに際して、必要なデータをどのようにして選択するのか、不明である。

ところでこのことは、受信したＳＩＧＮＡＬによっては、サーバは対応するクライアントを「特定」すなわち「識別」することができないということである。またステップＳ２ではＳＩＧＮＡＬの比較によりクライアントの正当性を判定しているが、このことは、ＳＩＧＮＡＬが「接続を要求してきたクライアントが何れのクライアントか」を判別するためには使用することができない一方で、「接続を要求してきたクライアントが正しいものか」を判定するために使用されるということである。すなわちＳＩＧＮＡＬとは「ＩＤ」というよりはむしろ「パスワード」としての機能を果たすものである。

また、クライアントがサーバの正当性を判定する際にサーバのＳＩＧＮＡＬを用いているが、クライアントはサーバに接続要求を出した時点で当該サーバを「識別」しているといえるから、サーバのＳＩＧＮＡＬがサーバの「ＩＤ」すなわち「識別情報」であるということも不明なことである。

そうすると、これらのＳＩＧＮＡＬがクライアントあるいはサーバの「ＩＤ」すなわち「識別情報」であるということは不明なことであるから、これらＳＩＧＮＡＬが「ワンタイムＩＤ」すなわち「一回限り使用可能な識別情報」であるとの明細書の記載は不明なものである。

（ｃ）実施の形態３には、ステップＰ２において、サーバがＳＩＧＮＡＬを演算により求め、受信したＳＩＧＮＡＬと照合することでクライアントを「識別」すると記載されている。しかしながら、（ｂ）で述べたと同様に、ＳＩＧＮＡＬを演算するにはクライアントに対応した情報が必要であるから、この演算の時点でクライアントが「特定」すなわち「識別」されていなければならない。そうすると、演算したＳＩＧＮＡＬと受信したＳＩＧＮＡＬとの照合でクライアントが「識別」されるということは、その意味するところが不明である。また、この照合による「識別」とは「接続を要求してきたものはいずれのクライアントであるのか」ということではなく、「接続を要求してきたものは正当なクライアントであるのか」ということであるならば、（ｂ）にて上述したようにＳＩＧＮＡＬとは「ＩＤ」ではなくむしろ「パスワード」に相当する情報であるというべきであるから、かかるＳＩＧＮＡＬが「ワンタイムＩＤ」であるということは不明である。クライアントにおけるサーバの「識別」についても同様のことがいえ、（ｂ）にて上述したようにクライアントはサーバに接続要求を出した時点で当該サーバを「識別」しているといえるから、サーバがクライアントに送信するＳＩＧＮＡＬについても、それが「ワンタイムＩＤ」であるということは不明である。

このことは実施の形態４，５，６，７についても同様である。

補充欄（いずれかの欄の大きさが足りない場合に使用すること）

第　Ⅷ　欄の続き

（ｄ）実施の形態８には、セッション回数ｎがクライアントに保持されている場合、ステップＳ６１，６２を省略できることが記載されている。しかしながら、これらのステップを省略した場合、サーバにクライアントのＩＤｃが通知されないから、ＳＩＧＮＡＬを求める際に、どのようにしてクライアントに対応した検証用情報を選択するのか不明である。またこのことにより、ＳＩＧＮＡＬが「ワンタイムＩＤ」であるということは（ｂ），（ｃ）で述べたと同様に不明なものである。

（ｅ）上述したように、実施の形態２－８として記載された発明においては、ＳＩＧＮＡＬによって受信側が送信側を「識別」することはできず、受信側が送信側が「認証」する際にＳＩＧＮＡＬをパスワードのごとく使用することが記載されているのみであるから、送信側の「識別」には、明細書に開示されていないＳＩＧＮＡＬとは別個の情報が必要であると認められる。そうすると、この出願の明細書には、請求の範囲１４－５０に記載された事項を十分に裏付ける記載がなされていないと認められる。

（ｆ）実施の形態４において、サーバがＳＩＧＮＡＬαクライアントがＳＩＧＮＡＬαを求めてサーバに送信することが記載されているが、サーバがそのＳＩＧＮＡＬαを用いて何らかの処理を行うということは何ら記載されていない。してみれば、クライアントがＳＩＧＮＡＬαを求めてサーバに送信することにどのような意味があるのか不明である。実施の形態５についても同様である。

（ｇ）実施の形態５において、クライアントがサーバに送信するＳＩＧＮＡＬαを「ワンタイムＩＤ」としている。しかしながら、ＳＩＧＮＡＬαの計算に用いる共有鍵Ｋは固定であり変化しないものであり、乱数Ｒ０を更新して変化させることも何ら記載されていないから、ＳＩＧＮＡＬαが通信毎に変化するものとは認められず、この点においても、ＳＩＧＮＡＬαが「ワンタイムＩＤ」であるということは不明なものである。またこのことによっても、この出願の明細書には、請求の範囲１６，１９，２５，４４，４５，４６に記載された事項を十分に裏付ける記載がなされていないといえる。

補充欄（いずれかの欄の大きさが足りない場合に使用すること）

第　Ⅲ　欄の続き

請求の範囲１の「生成した新規の記憶データを前記履歴データを用いて暗号化して第２認証装置に送信する」との記載における「生成した新規の記憶データ」が、「前記第１認証装置は、記憶されている履歴データを用いて記憶データを新規に生成し」との記載における「記憶データ」と同一のデータであるのか否か不明であり、同様に、「生成した新規の記憶データを前記履歴データを用いて暗号化して第１認証装置に送信する」との記載における「生成した新規の記憶データ」が、「前記第２認証装置は、…記憶されている履歴データを用いて記憶データを新規に生成し」との記載における「記憶データ」と同一のデータであるのか否かという点も不明である。また、それぞれ別個のデータであるならば、履歴データを用いて記憶データを生成することにどのような意味があるのか不明である。同じく、「前記第２認証装置は、前記第１認証装置からの記憶データ…を用いて新規に記憶データを生成し」との記載における「第１認証装置からの記憶データ」とは、「生成した新規の記憶データを…暗号化して第２の認証装置に送信する第１送信工程」との記載における「記憶データ」と同一のデータであるのか否か不明であり、異なるデータであるならば、「第１認証装置からの記憶データ」とは、如何なるデータであるのか不明である。

さらに「前記第１認証装置は、記憶されている履歴データを用いて記憶データを新規に生成し」及び「前記第２認証装置は、…記憶されている履歴データを用いて記憶データを新規に生成し」と記載されているが、各々、「前回の認証による記憶データを用いて更新した更新結果を履歴データとして」との記載における「履歴データ」と同一のデータであるのか不明であり、異なるデータであるならば、これらの記載における「履歴データ」及びその後の記載における「前記履歴データ」とは、如何なるデータであるのか不明である。

また「前回の認証による記憶データを用いて更新した更新結果を履歴データとして」との記載における「前回の認証による記憶データ」とは如何なるものかということも不明である。

すなわち請求の範囲１に記載された「相互認証方法」については、複数存在する「記憶データ」及び「履歴データ」の間の関係が不明であるため、どのような手順にて認証が行われているのか把握することができない。請求の範囲１を引用する請求の範囲２－１３についても同様である。

ただし、m≧1の自然数である。

また、クライアント・コンピュータ10側の暗証データC、及びサーバ・コンピュータ40側の暗証データSを他方へ送信するが、以下に説明するように、暗証データは情報授受の度に変更している。すなわち、クライアント・コンピュータ10からサーバ・コンピュータ40へ送信する暗証データCは、その送信するときに予め定めた関数y（S，R）により新規の暗証データCを生成して送信する。関数yは、単純和や係数付加の多項式、乗算、積和そしてハッシュ関数が一例としてある。同様に、サーバ・コンピュータ40からクライアント・コンピュータ10へ送信する場合も、予め定めた関数z（C，Q）により暗証データSを生成して送信する。関数zは、単純和や係数付加の多項式、乗算、積和そしてハッシュ関数が一例としてある。次に、関数y、zの一例を示す。

$C_m = y(S, R) = S_{m-1} + R_{m-1}$

$S_m = z(C, Q) = C_m + Q_{m-1}$

ただし、m≧1の自然数である。

なお、暗証データの送信では、第三者による特定を困掛こするため、秘匿してもよい。例えば、クライアント・コンピュータ10からサーバ・コンピュータ40へ送信する暗証データC、及びサーバ・コンピュータ40からクライアント・コンピュータ10へ送信する暗証データSを隠蔽鍵Kで隠蔽するようにしてもよい。すなわち、隠蔽鍵Kをパラメータとして追加した関数にしてもよい。

（詳細プロセス）

図4は本発明の第1の実施の形態に係る相互認証における詳細プロセスを示すイメージ図である。以下、図4を参照して本実施の形態の詳細プロセスを説明する。

ステップP0：クライアント・コンピュータ10及びサーバ・コンピュータ40の各々に、初期値の隠蔽鍵K。を格納する。このプロセスは、図3のステップ100と、図4のプロセスPc0及びPs0に相当する。

ステップP1：クライアント・コンピュータ10では、乱数Rを生成し、暗証データC及び認証データAを計算し、サーバ・コンピュータ40に送信する。こ

上記第一装置が、上記第一の乱数、上記第二の乱数および上記共有鍵を引数とする一方向関数の関数値を第三のワンタイムＩＤとして求め、この第三のワンタイムＩＤを上記第二装置に対して送信するステップと、

上記第二装置が、上記第一の乱数、上記第二の乱数および上記共有鍵に基づいて上記第三のワンタイムＩＤを演算により求め、この演算結果と上記第一装置から受信した上記第三のワンタイムＩＤとの比較により、上記第一装置の正当性を判定するステップとを有することを特徴とする認証方法。

２６．　上記第一の乱数と上記第二の乱数を、上記第一装置と上記第二装置との間で予め共有化された共有鍵で暗号化した状態で、送信するようにしたことを特徴とする請求項２４に記載の認証方法。

２７．（補正後）上記第一の乱数と上記第二の乱数を、上記第一装置と上記第二装置との間で予め共有化された共有鍵で暗号化した状態で、送信するようにしたことを特徴とする請求項２５に記載の認証方法。

２８．　上記第二装置が上記第二のワンタイムＩＤと上記第二の乱数とを上記第一装置に対して送信するステップにおいて、上記第二装置は、上記第一装置との間で予め共有化された乱数を初期乱数として、この初期乱数と上記第一の乱数を引数とする所定の演算を行い、この演算結果を上記第一装置に対して送信する一方、上記第一装置は、上記第二装置の正当性の判定材料として、上記第二装置から受信した上記演算結果を、上記第二のワンタイムＩＤとともに用いることを特徴とする請求項２４乃至請求項２６の何れかに記載の認証方法。

２９．　上記第一装置が上記第三のワンタイムＩＤを上記第二装置に対して送信するステップにおいて、上記第一装置は、上記第一の乱数と上記第二の乱数を引数とする所定の演算を行い、この演算結果を上記第二装置に対して送信する一方、上記第二装置は、上記第一装置の正当性の判定材料として、上記第一装置から受信した上記演算結果を、上記第三のワンタイムＩＤとともに用いることを特徴とする請求項２４に記載の認証方法。

３０．　上記第一装置が上記第三のワンタイムＩＤを上記第二装置に対して送信するステップにおいて、上記第一装置は、上記第一の乱数と上記第二の乱数